

Table of Contents

Invited Contribution

| | |
|--|---|
| On the Construction of Automata from Linear Arithmetic Constraints | 1 |
| <i>Pierre Wolper and Bernard Boigelot</i> | |

Software and Formal Methods Tools

| | |
|--|----|
| An Extensible Type System for Component-Based Design | 20 |
| <i>Yuhong Xiong and Edward A. Lee</i> | |
| Proof General: A Generic Tool for Proof Development | 38 |
| <i>David Aspinall</i> | |
| ViewPoint-Oriented Software Development: Tool Support for Integrating Multiple Perspectives by Distributed Graph Transformation | 43 |
| <i>Michael Goedicke, Bettina Enders, Torsten Meyer and Gabriele Taentzer</i> | |

Formal Methods Tools

| | |
|--|----|
| Consistent Integration of Formal Methods | 48 |
| <i>Peter Braun, Heiko Lötzbeyer, Bernhard Schätz and Oscar Slotosch</i> | |
| An Architecture for Interactive Program Provers | 63 |
| <i>Jörg Meyer and Arnd Poetzsch-Heffter</i> | |
| The PROSPER Toolkit | 78 |
| <i>Louise A. Dennis, Graham Collins, Michael Norrish, Richard Boulton, Konrad Slind, Graham Robinson, Mike Gordon and Tom Melham</i> | |
| CASL: From Semantics to Tools | 93 |
| <i>Till Mossakowski</i> | |

Timed and Hybrid Systems

| | |
|---|-----|
| On the Construction of Live Timed Systems | 109 |
| <i>Sébastien Bornot, Gregor Gößler and Joseph Sifakis</i> | |
| On Memory-Block Traversal Problems in Model-Checking Timed Systems | 127 |
| <i>Fredrik Larsson, Paul Pettersson and Wang Yi</i> | |
| Symbolic Model Checking for Rectangular Hybrid Systems | 142 |
| <i>Thomas A. Henzinger and Rupak Majumdar</i> | |

| | |
|--|-----|
| Efficient Data Structure for Fully Symbolic Verification of Real-Time Software Systems | 157 |
| <i>Farn Wang</i> | |

Infinite and Parameterized Systems

| | |
|---|-----|
| Verification of Parameterized Systems Using Logic Program Transformations | 172 |
| <i>Abhik Roychoudhury, K. Narayan Kumar, C.R. Ramakrishnan, I.V. Ramakrishnan and Scott A. Smolka</i> | |

| | |
|--|-----|
| Abstracting WS1S Systems to Verify Parameterized Networks | 188 |
| <i>Kai Baukus, Saddek Bensalem, Yassine Lakhnech and Karsten Stahl</i> | |

| | |
|--|-----|
| FMona: A Tool for Expressing Validation Techniques over Infinite State Systems | 204 |
| <i>J.-P. Bodeveix and M. Filali</i> | |

| | |
|---|-----|
| Transitive Closures of Regular Relations for Verifying Infinite-State Systems | 220 |
| <i>Bengt Jonsson and Marcus Nilsson</i> | |

Diagnostic and Test Generation

| | |
|--|-----|
| Using Static Analysis to Improve Automatic Test Generation | 235 |
| <i>Marius Bozga, Jean-Claude Fernandez and Lucian Ghirvu</i> | |
| Efficient Diagnostic Generation for Boolean Equation Systems | 251 |
| <i>Radu Mateescu</i> | |

Efficient Model-Checking

| | |
|---|-----|
| Compositional State Space Generation with Partial Order Reductions for Asynchronous Communicating Systems | 266 |
| <i>Jean-Pierre Krimm and Laurent Mounier</i> | |

| | |
|--|-----|
| Checking for CFFD-Preorder with Tester Processes | 283 |
| <i>Juhana Helovuo and Antti Valmari</i> | |

| | |
|---|-----|
| Fair Bisimulation | 299 |
| <i>Thomas A. Henzinger and Sriram K. Rajamani</i> | |

| | |
|---|-----|
| Integrating Low Level Symmetries into Reachability Analysis | 315 |
| <i>Karsten Schmidt</i> | |

Model-Checking Tools

| | |
|--|-----|
| Model Checking Support for the ASM High-Level Language | 331 |
| <i>Giuseppe Del Castillo and Kirsten Winter</i> | |

| | |
|---|-----|
| A Markov Chain Model Checker | 347 |
| <i>Holger Hermanns, Joost-Pieter Katoen, Joachim Meyer-Kayser and Markus Siegle</i> | |
| Model Checking SDL with Spin | 363 |
| <i>Dragan Bošnački, Dennis Dams, Leszek Holenderski and Natalia Sidorova</i> | |
| Salsa: Combining Constraint Solvers with BDDs for Automatic Invariant Checking | 378 |
| <i>Ramesh Bharadwaj and Steve Sims</i> | |

Symbolic Model-Checking

| | |
|--|-----|
| Symbolic Model Checking of Probabilistic Processes Using MTBDDs and the Kronecker Representation | 395 |
| <i>Luca de Alfaro, Marta Kwiatkowska, Gethin Norman, David Parker and Roberto Segala</i> | |
| Symbolic Reachability Analysis Based on SAT-Solvers | 411 |
| <i>Parosh Aziz Abdulla, Per Bjesse and Niklas Eén</i> | |
| Symbolic Representation of Upward-Closed Sets | 426 |
| <i>Giorgio Delzanno and Jean-François Raskin</i> | |
| BDD vs. Constraint-Based Model Checking: An Experimental Evaluation for Asynchronous Concurrent Systems | 441 |
| <i>Tevfik Bultan</i> | |

Visual Tools

| | |
|--|-----|
| Tool-Based Specification of Visual Languages and Graphic Editors | 456 |
| <i>Magnus Niemann and Roswitha Bardohl</i> | |
| VIP: A Visual Editor and Compiler for v-Promela | 471 |
| <i>Moataz Kamel and Stefan Leue</i> | |

Verification of Critical Systems

| | |
|---|-----|
| A Comparison of Two Verification Methods for Speculative Instruction Execution | 487 |
| <i>Tamarah Arons and Amir Pnueli</i> | |
| Partial Order Reductions for Security Protocol Verification | 503 |
| <i>Edmund Clarke, Somesh Jha and Will Marrero</i> | |
| Model Checking Security Protocols Using a Logic of Belief | 519 |
| <i>Massimo Benerecetti and Fausto Giunchiglia</i> | |

A Formal Specification and Validation of a Critical System in
Presence of Byzantine Errors 535
S. Gnesi, D. Latella, G. Lenzini, C. Abbaneo, A. Amendola and P. Marmo

Author Index 551

Tools and Algorithms for the Construction and Analysis
of Systems

6th International Conference, TACAS 2000 Held as Part
of the Joint European Conferences on Theory and
Practice of Software, ETAPS 2000 Berlin, Germany,
March 25 - April 2, 2000 Proceedings

Graf, S.; Schwartzbach, M. (Eds.)

2000, XIV, 552 p., Softcover

ISBN: 978-3-540-67282-1